IN THE CLAIMS:

1. A method enabling a user in a mobile environment to conduct transactions via a self-service merchant terminal, comprising:

a) maintaining a security key in a mobile phone device;

b) imprinting at least an association of the security key and a mobile phone identification into at least one associated portable pilot;

c) transferring at least the association of the security key and the mobile phone identification from the pilot to a self-service merchant terminal through an initial short-range radio link; and

d) establishing a secure short-range connection between the self-service terminal and the mobile phone based on the transferred security key and the mobile phone identification information, wherein the initial short-range radio link has a significantly smaller radio coverage than the secure short-range connection.

2. The method of claim 1, wherein the secure short-range connection is used to conduct transactions without using currency.

3. The method of claim 1, wherein the initial short-range radio link complies with RFID technology.

4. The method of claim 1, wherein the secure short-range connection complies with Bluetooth technology.

5. The method of claim 1, wherein the coverage area of the short-range radio link is under 10 centimeters.

6. The method of claim 1, wherein the mobile phone identification is a Bluetooth address of the mobile phone.

7. The method of claim 1 further comprising:

e) receiving a user transaction interface at the terminal upon establishment of the secure short-range connection.

8. The method of claim 1 further comprising:

f) providing the at least one pilot a random number and a sequence number (SEQ) in response to a request for a secure connection between the terminal and the device.

9. The method of claim 1 further comprising:

g) computing a RES=f (random number, SEQ, secret key (k)) and session key K' by the pilot and sending the RES and K' to the terminal.

10. The method of claim 1 further comprising:

h) using the session key by the terminal to establish the secure connection with the device.

11. The method of claim 1 further comprising:

i) deriving the session key by the device and using the derived session key for secure short-range communication with the terminal.

12. The method of claim 1 further comprising:

j) verifying the presence of a correct pilot by the terminal via computing an expected response of XRES=f (random number, SEQ, K) and verifying whether RES=XRES.

13. The method of claim 1 further comprising:

k) using symmetric keys for encryption/decryption of information transferred between the terminal and the device.

14. The method of claim 1 further comprising:

l) using public key infrastructure for encryption/decryption of information transferred between the terminal and the device.

15. The method of claim 1 further comprising:

m) storing a plurality of authentication codes in the at least one pilot for one time use in initiating secure connection requests.

16. The method of claim 1further comprising:

n) storing a plurality of authentication codes for one time use in the device for establishing short-range connections between the device and the terminal.

17. The method of claim 1 further comprising:

o) transferring payment information from the terminal to the device via the secure channel based upon a session key K';

p) automatically accepting the payment information by the device; and

q) using a communication channel either provided by the terminal or the device to conduct a transaction.

18. The method of claim 1 further comprising:

r) sending a request to the device by the terminal for the device to launch a payment application;

s) launching the payment application after the device verifies the presence of a correct pilot;

t) using the payment application at the terminal to launch a legacy payment client; and

u) finalizing the transaction by a user at a user-interface displayed at the terminal.

19. A system for enabling a user in a mobile environment to conduct transactions via a self-service terminal, comprising:

a) a mobile device including a short-range communication transceiver and an RFID transceiver;

b) a portable pilot device associated with the mobile device and including a semi-passive RFID transponder;

c) a self-service terminal including a RFID transceiver and a short-range transceiver;

d) means for storing identification information and at least security information in the mobile device;

e) means for imprinting said stored identification and at least an association of the security information of the device over an RFID connection into the associated portable pilot;

f) means for transferring by the pilot said imprinted identification and security information to the self-service terminal over an RFID connection; and

g) means for establishing a secure short-range connection between the self-service terminal and the device based on said transferred identification and security information of the device, wherein the RFID connection has significantly smaller radio coverage than the secure short-range connection.

20. The system of claim 19, wherein the secure short-range connection is used to conduct transactions without using currency.

21. The system of claim 19 wherein the self-service terminal receives a user transaction interface upon establishment of the secure connection.

22. The system of claim 19 further comprising:

h) means for storing a plurality of authentication codes for one time use in establishing a connection between the pilot and the device.

23. The system of claim 19 further comprising:

i) means for storing a plurality of authentication codes for one time use in establishing short-range connections between the device and the terminal.

24. The system of claim 19 wherein the pilot identifies the device for a short-range connection and initializes a security context.

25. The system of claim 19 wherein the user operates the user transaction interface at the terminal.

26. The system of claim 19 further comprising:

j) means activating the terminal for establishing a secure connection to the device.

27. Apparatus enabling a user in a mobile environment to activate a self-service terminal to conduct transactions, comprising:

a) a semi-passive transponder for responding to RF signals transmitted by an associated mobile device;

b) a memory coupled to the transponder;

c) a processor coupled to the transponder and the memory; and

d) means responsive to the transponder for storing unique information related to a mobile device.

28. The apparatus of claim 27 comprising:

e) means for transmitting the stored information to the self-service terminal after activation from the terminal.

29. The apparatus of claim 27 further comprising:

f) means for exchanging authentication information with a mobile device for receiving the unique information related to the mobile device to be provided to the self-service terminal for initiating a secure connection between the mobile device and the self-service terminal.

30. The apparatus of claim 27 further comprising:

g) means for exchanging authentication information with the self-service terminal for initiating a secure connection between the mobile device and the self-service terminal..

31. The apparatus of claim 27 further comprising:

h) means for storing a plurality of authentication codes for one time use in establishing a connection between the pilot and the device.

32. The apparatus of claim 27 further comprising:

i) means for identifying the device for a short-range connection between the terminal and the device and initializing a security context.

33. A medium, executable in a computer system, enabling a user in a mobile environment to activate a self-service terminal to conduct transactions, the medium comprising:

a) program code for storing at least a security key in a mobile phone device;

b) program code for imprinting at least an association of the security key and mobile phone device identification in a portable pilot associated with the mobile phone device;

c) program code for transferring at least the association of the security key and mobile phone device identification from the pilot to a self-service terminal through an initial short-range radio link; and

d) program code for establishing a secure short-range connection between the self-service terminal and the mobile phone device for conducting transactions based on the transferred security key and mobile phone device identification, wherein the initial short-range link has a significantly smaller radio coverage than the secure short-range connection.

34. The medium of claim 33 further comprising:

e) program code in the terminal for downloading a user interface from the mobile phone device after establishment of a secure connection with the mobile phone device.

35. The medium of claim 33 further comprising:

f) program code for conducting product or service transactions between the terminal and the mobile phone device without using currency.

36. The medium of claim 33 wherein the terminal is within a merchant establishment or in a kiosk.

37. A method of enabling a first pilot device to serve as a master pilot for at least one second pilot devices as slave devices capable of interacting with a terminal, comprising:

installing a reader and switching means in the first pilot device serving as a master device and further including a processor and storage means;

Imprinting and storing in the master pilot device a phone address and a security key of a mobile phone;

At least one second pilot device, each serving as a slave device to the master device and further including a processor and storage, each slave device capable of receiving and transmitting signals from/to the master device;

Imprinting the phone address, security key and policy restraints in a slave device after receiving an address identifying the slave device; and

using the slave device to interact with a terminal to purchase an item, after a secure connection is established between the terminal and the mobile phone.

38. The method of claim 37, wherein the imprinting step further comprises:

limiting the validity of the at least one portable pilot based on a predefined policy constraint.

39. The method of claim 37, wherein the predefined policy constraint includes at least one of a maximum purchase value and a maximum time limit.

40. The method of claim 37 further comprising:

storing a list of prohibited purchase items in the slave device.

41. The method of claim 37 further comprising:

transmitting a list of purchased items from the terminal to the slave device.

42. The method of 37 further comprising:
comparing the purchased items to prohibited items stored in the slave device.

43. The method of claim 37 further comprising:
verifying in the slave device that no purchased item is a prohibited item.

44. The method of claim 37 wherein a policy restraints limits usage of the slave device to a maximum value for a purchased item.

45. The method of claim 37 wherein the policy restraints limits usage of the slave device to a maximum time period.

46. The method of claim 37 wherein the terminal receives a signal from the slave indicating approval or denial of a purchased item.

47. The method of claim 37 wherein the terminal displays approval or denial of the purchased items after receiving a signal from the slave device.

48. The method of claim 37 wherein the slave device touches or holds the slave device in close proximity to the terminal to authorize payment for the purchased after the terminal displays approval of the purchased by the slave device.